METHOD FOR THE ENCRYPTION AND DECRYPTION OF DATA BY VARIOUS USERS

[0001] The present application hereby claims priority under 35 U.S.C. §119 on German patent application number DE 103 07 996.3 filed February 25, 2003, the entire contents of which are hereby incorporated herein by reference.

Field of the Invention

[0002] The invention generally relates to a method for the encryption and decryption of data by various users. The invention also generally relates to a data processing facility for carrying out the method and to a storage medium which stores information, e.g. a computer program, for carrying out the method.

Background of the Invention

[0003] The increased use of electronic data and communication channels entails constantly growing demands on the protection of data against unwanted data access, but also simultaneously on the ability to access data with the greatest of ease, convenience and the least complexity possible. Particularly on account of the increasing reciprocal networking and the frequently large number of different users who are able to gain physical access to particular data, effective electronic or software-based control and protective mechanisms have become indispensable.

[0004] The effective protection of data which can be accessed in diverse ways against unauthorised access plays a significant role. A large number of encryption mechanisms using symmetrical or asymmetrical data keys are known, of which the encryption programs such as

PGP, which operate on the basis of asymmetrical key systems, are probably among the securest and most convenient to handle and are therefore used most widely. Both symmetrical and asymmetrical key systems are based on the use of at least one individual data key, which must be accessible only to the authorised user for the purpose of encrypting and decrypting his data. Access to this individual key needs to be protected from unauthorised users as effectively as possible.

[0005] The protection of electronic data from unauthorised access plays a particularly significant role for person-related data such as address lists or customer data, for data in the financial sector and particularly for data in the health sector. In the health sector, where the most stringent demands are placed on data integrity, data protection provisions demand that any user of data be clearly identified and authenticated. Authentication refers to a user's authentication being awarded on the basis of his identification, wherein only authenticated users can obtain access to the data in question. In the health sector, the authentication function is also called "access control".

[0006] In addition to authentication, in security-critical data applications, e.g. in telemedicine or in home care systems, any communication over fundamentally nonsecure communication channels and any storage of security-critical data require encryption. When using encrypted data, it may be necessary for a plurality of different users to be able to access the data. This may be the case, by way of example, when customer data are being managed by the employees of a bank, in the case of personal data in personnel departments, in the case

of joint use of data in development teams or in the case of data in the health sector which should be accessible to a plurality of treating physicians or to a particular group of medical specialist personnel. In this case, there is the problem that data which have been encrypted by a particular user using his individual data key cannot be decrypted by other users using other individual data keys.

[0007] To make the encrypted data available nevertheless to particular user groups for the purpose of joint use, it is often customary to communicate the data key required for this purpose to all users. Distributing the key to the user group causes considerable problems for data integrity, since the key needs to be communicated to a large number of people who are involved, and since the fact that it is difficult to memorise data keys which are effective for security purposes means that it is not unusual for these data keys to be kept in an inappropriate manner, e.g. on notepaper in desk drawers. The central management of the keys also makes it necessary to keep key logs, "code logs", whose ability to be spied out represents a further security problem factor.

SUMMARY OF THE INVENTION

[0008] An object of an embodiment of the invention is to simplify the secure handling of data keys for a plurality of different users for the purpose of using common encrypted data.

[0009] An embodiment of the invention achieves an object by a method, by an apparatus and/or by a storage medium having information, e.g. a computer program, for carrying out the method.

[0010] An embodiment of the invention is based on the insight that the ability to encrypt and decrypt jointly used data is not person-related, but rather group-related. Each user of the encrypted data for joint use is thus no longer identified as person but rather on the basis of his association with a group.

[0011] A basic concept of an embodiment of the invention involves people who have joint use of encrypted data not being assigned user-specific data keys for accessing the data. Instead, such people are assigned a common user group data key on the basis of their association with a user group. All members of the user group can use the user group data key to encrypt and decrypt data which are intended for joint use. The data key is automatically assigned but is not communicated to the users, i.e. the users receive no knowledge of the actual nature of the data key. Accordingly, they neither need to remember the data key nor are they able to communicate it. This rules out significant security problem factors associated with conventional key systems.

[0012] In addition, this affords the further advantage that changes in the personnel making up a user group do not necessitate changes to the data key. In particular, it is not necessary to introduce a new data key when individual people leave the user group, since these people have no knowledge of the nature of the data key which they might misuse in some way after they have left the group. Instead, they are simply no longer assigned a valid data key if they attempt to access data.

[0013] In addition, the use of an automatically assigned user group data key means that the data key can be made

as complex as desired and can be changed as often as desired. It is down to the encryption system to recode the encrypted data stocks automatically, i.e. to decrypt them using the old data key, to encrypt them again using the new data key, and to assign the new user group data key to the users at a time appropriate to the conversion. This eliminates any complexity for communicating the new data key and for timing its introduction, which rules out further risks to the security of the encryption system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] The present invention will become more fully understood from the detailed description of preferred embodiments given hereinbelow and the accompanying drawings, which are given by way of illustration only and thus are not limitative of the present invention, and wherein:

FIGURE 1 shows a flowchart with the method steps required for implementing an embodiment of the invention,

FIGURE 2 shows a system architecture which is suitable for implementing an embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0015] Figure 1 shows the method steps which are required for implementing an embodiment of the invention. The method starts in step 1 by requiring data access which necessitates the use of a cryptography program for the encryption or decryption of data. In step 3, the cryptography program is started. Depending on the

application, the cryptography program can be started by the user himself or can be started automatically from an application program.

[0016] In step 5, a security check is performed which is intended to be used to identify the user as a really existing person. To this end, the user is asked for person-specific data which must satisfy all the demands on data integrity. Preferably, the security check is performed by way of biometric detection of characteristic data which are as deception-proof as possible, such as a finger print or a form of the iris. It is also possible for the user to identify himself using an electronic chip card or using an electronic or mechanical key.

[0017] In step 7, the cryptography program accesses a user database. The user database stores information which can identify the user using the data which has previously been ascertained in the security check in step 5.

[0018] In step 9, the cryptography program takes the data from the security check and the data from the user database check as a basis for ascertaining the identity of the user. The degree of proof against deception when ascertaining the user identity is in this case essentially dependent on the security check's proof against deception in step 5 and also on the data integrity of the user database.

[0019] In step 11, the cryptography program checks a user group database. This contains data which allow the user to be assigned to a user group on the basis of his previously ascertained user identity. The user group database thus contains information about groups of

users having the same level of authorisation. Such groups can be, for example, practice teams made up of medical specialist personnel, members of financial institutes, members of personnel departments or research teams. A common feature of all of these groups is that they work with the same person-specific or object-specific, security-critical data, which although they must be accessible to all team members, must under no circumstances be able to accessed elsewhere.

[0020] Association with a group can be obtained either on an object-related basis, i.e. from the need for particular users to be able to work with a particular data stock, or on a subject-related basis, i.e. from the respective user's hierarchic authorisation or confidentiality classification allowing him basic access to data on a particular security level on the basis of his position in the organisation. Furthermore, a user may belong to a plurality of user groups representing, by way of example, a plurality of practice teams in which the user is simultaneously collaborating. In such cases, the user automatically has access to various, different data stocks.

[0021] In step 15, the cryptography program checks a data key database. The data key database contains information which allows particular data keys to be assigned to particular users or user groups.

[0022] In step 17, the cryptography program ascertains the data key(s) to be assigned from the previously ascertained user group and the data in the data key database.

[0023] In step 19, the cryptography program notifies the respective user of his data key(s). This process takes

place without being able to be viewed by the user, since the cryptography program uses the ascertained data key(s) directly for encrypting or decrypting application data. In particular, the user is provided with no information about the nature of the assigned data keys. One or more data key(s) is/are assigned automatically and unnoticed by the user as the result of the security check.

[0024] In step 21, the cryptography program performs the requested cryptographical operation, that is to say it encrypts or decrypts data for use by the user or by another application program started by the user. In step 23, the complete cryptography process has ended and the user is logged off from the encryption system again.

[0025] The method for carrying out an embodiment of the invention has been described on the basis of the use of three different databases, a user database, a use group database and a data key database. The three databases represent the logical associations between information which need to be made in the course of the encryption method. First, the user needs to be identified as the result of the security check; secondly, the identified user needs to be associated with a user group; and thirdly, the data key belonging to this user group needs to be ascertained.

[0026] The use of three databases gives the encryption system a modular structure with the greatest possible flexibility. Changes can be made in each of the three databases at any time independently of the other two databases. In the user database, it is possible to change the security-critical information used to identify the user on a regular basis. In the user group

database, it is possible to make changes to the groups, that is to say to the people intended to have joint use of data stocks, which reflect actual changes in the association between individual people and user teams. In the data key database, changes can be made to the data keys on a regular basis in order to increase the security of the system. In this connection, it is respectively necessary to recode the data stock, i.e. to decrypt it using the old data key and to encrypt it with the new data key which is to be introduced.

[0027] Although the modular structure with three databases correctly represents the actual logical associations, it is naturally possible to use just two or else just one database system instead.

[0028] Figure 2 shows an electronic data processing facility 31 on which the method for implementing an embodiment of the invention can be carried out. The data processing facility 31 has a keyboard 33 or other input unit and also a screen 35. Depending on the type of application, audible input and output signals can also be processed. The type and scope of the input and output units are of no importance to the implementation of the invention. The data processing facility has access to an application data store 37 which is used for storing preferably encrypted application data. The electronic data processing facility can either be a medical workstation, e.g. a "modality", or any other workstation with a screen, e.g. a bank terminal.

[0029] The data processing facility 31 is connected to a security check device 39 which is used to ascertain data for the purpose of identifying the respective user. The security check device 39 can include a chip card reader which reads a user-specific chip card. It

may also be a mechanical or electronic lock requiring a user-specific key. Not least, it may be a sensor for ascertaining biometric data from the user, for example measuring the form of the user's iris, his fingerprints or his voice frequency range. The use of biometric data for the security check has the advantage that it is not necessary to use any kind of key or card which the user might lose or which might be stolen from him. In addition, biometric data's proof against deception can be regarded as being higher than that of other key systems.

[0030] The data processing facility 31 also has access to a user data store 41 which contains information for identifying users on the basis of the data ascertained by the security check means 39. These data allow the system to identify the respective user as a really existing person.

[0031] The data processing facility 31 also has access to a user group data store 43 which contains data which can be used to establish association between users and user groups. By checking these data, the system is able to establish that user group or those user groups to which a previously identified user belongs.

[0032] The data processing facility 31 also has access to a data key data store 45 which contains data which can be used to find data keys assigned to users and user groups. The data key data store obviously contains the most security-critical information in this system in as much as it contains all the data keys which can be used to decrypt data in the application data store 37.

[0033] For the data key data store 45, particular security requirements apply which can make it

appropriate for this data store to be set up centrally at a remote location. For this purpose, the data processing facility 31 accesses the data key data store 45 using a data telecommunication device 47. The remote placement of the data key data store 45 firstly allows it to be isolated from the data processing facility 31 and hence allows the isolation of any other data processing facilities which may be networked to the data processing facility 31. Secondly, it allows particularly stringent security precautions to be put in place specifically for the data key data store 45, such as particularly restrictive firewalls.

[0034] Depending on security precautions, the data telecommunication device 47 can have a protected or an unprotected communication channel. In addition, the communication channel for the data telecommunication device 47 may be completely disabled and may be opened only on the basis of the result of the security check by the security check device 39; this can be done using a telephone modem connection, for example.

[0035] Depending on the organisation of the work which is to be carried out using the data processing facility, the various data stores 37, 41, 43, 45 may all be separate or may be partially or fully combined. Dispensing with the modular structure having individual data stores and with the remote arrangement of the data key data store 45, it is possible, by way of example, for all the relevant data to be stored in a single local memory in the data processing facility 31, e.g. its hard disk. On the other hand, by way of example, the user group data store 43 may have been set up in a management department which is responsible for organising the workflows and for compiling the user groups, whereas the data key data store 45 may be in an

information technology department which is responsible for implementing and realising the encryption system, and finally the user data store 41 may be in an identification location which is responsible for personal data and for detecting and verifying person-specific identification or security data.

[0036] The only fundamental aspect of the electronic data processing facility for implementing an embodiment of the invention is that the security check by the security check device 39 allows no inference of the data key which the encryption system uses to encrypt and decrypt application data. This isolation forms the basis for the ability to assign a data key for encrypting and decrypting data which evades direct access by the user and cannot be viewed by him. Instead, the user uses a single logon process on the system for the purpose of automatically obtaining the data key(s) defined by his group association for the purpose of accessing the encrypted data.

[0037] Exemplary embodiments being thus described, it will be obvious that the same may be varied in many ways. Such variations are not to be regarded as a departure from the spirit and scope of the present invention, and all such modifications as would be obvious to one skilled in the art are intended to be included within the scope of the following claims.